３．サーバルームに関する標準

0.91 版

---------- 取扱注意事項 ----------

特定非営利活動法人日本ネットワーク・セキュリティ協会（JNSA）のセキュリティポリシーワーキンググループにて作成した「情報セキュリティポリシーサンプル」(以下、ポリシーサンプル)をご参照、ご利用される場合、以下の事項に従ってください。

1. 公開の目的

1-1. セキュリティポリシーを作成する際の参考

1-2. 既存のセキュリティポリシーとの比較によるレベル向上

1-3. 既存のセキュリティレベルの大まかな把握

2. ご利用にあたっての注意事項

2-1. ポリシーサンプルの版権は、NPO 日本ネットワークセキュリティ協会（JNSA）に属します。

2-2. ポリシーサンプルへのリンクは、JNSA 事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ず JNSA サイトのトップページ(http://www.jnsa.org/)を指定してください

2-3. ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG 作成ポリシーサンプル」を明記して下さい。営利目的、非営利目的の区別はありません。

ポリシーサンプルの全部あるいは一部をそのまま、ご使用いただく場合：

【出典】「情報セキュリティポリシーサンプル(0.91 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

ポリシーサンプルを一部加工して、ご使用いただく場合：

【参考文献】「情報セキュリティポリシーサンプル(0.91 版)」
NPO 日本ネットワークセキュリティ協会(JNSA) http://www.jnsa.org/

2-4. ポリシーサンプルを利用したことによって生ずるいかなる損害に関しても JNSA は一切責任を負わないものとします。

2-5. 本ポリシーサンプルを報道、記事など、メディアで用いられる場合には、JNSA 事務局にご一報ください。

3. ご意見等連絡先

ポリシーサンプルに関するご意見・ご感想・ご質問等がありましたら、JNSA 事務局まで E-Mail にてご連絡ください。ただし勧誘、商品広告、宗教関連、チェーンメールの E-Mail はお断りします。

また、E-Mail にファイルを添付する場合は、添付するファイルをアンチウイルスソフトウエア等で予め検査を行ってください。

URL：http://www.jnsa.org　E-Mail：sec@jnsa.org

３．サーバルームに関する標準

３．１　趣旨

本標準は、サーバルームの設置によってサーバ等を保護し、それらに格納する情報の安全性を確保することを目的とする。

３．２　対象者

サーバルームの設置と利用に関わるすべての従業員

３．３　対象システム

サーバルームに設置するサーバ及びその他の機器

３．４　遵守事項

３．４．１　サーバルームの定義

（１）　サーバルームの定義は「重要度の高い情報資産が格納されているサーバがまとめて設置される部屋」とする。重要度の高い情報資産については別途定める。

（２）　電子化されたデータとして保存する重要度の高い情報資産は、『クライアント等におけるセキュリティ対策標準』および『媒体の取り扱いに関する標準』に基づいて管理される場合を除き、サーバルームに設置するサーバでのみ保存されなければならない。

３．４．２　サーバルームの物理的セキュリティ

（１）　サーバルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスとの隣接は避けなければならない。

（２）　サーバルームは、危険物保管場所、火気施設、水道設備等、災害のリスクの大きい場所からは遠ざけて設置しなければならない。

（３） サーバルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。

（４） サーバルームの出入り口は原則１ヶ所に限定し、施錠設備を設けなければならない。

（５） サーバルームに窓を設けることは極力避け、設ける場合は網付きガラス・強化ガラス等を用いなければならない。

（６） サーバルームには設置する機器・設備の重要度に応じて、防犯カメラ、侵入報知機等の防犯設備の設置を検討しなければならない。

（７） サーバルームには必要に応じて、非常電話、非常ベル等の非常用連絡設備の設置を検討しなければならない。

（８） サーバルームにはコピー・FAX 等の設備を設置してはならない。

（９） その他のサーバルームの物理的セキュリティについては『物理的対策標準』でのセキュリティ区画の扱いに準ずる。

３．４．３　サーバルームの運用

（１） サーバルームは従業員不在時には施錠しなければならない。

（２） サーバルームおよびその鍵の管理については管理責任者を置かなければならない。

（３） サーバルームへの入室は、受付または認証装置（入館カード、パスワード入力、生体認証）等によって特定の登録メンバに制限されなければならない。

（４） サーバルームへの未登録者の入室および作業実施については管理責任者の許可と登録メンバの同伴がなければならない。

（５） サーバルームに入室可能な登録メンバは定期的に見直さなければならな

い。

（６） サーバルームに入室不要となった登録メンバは速やかに登録を解除し、入室のための認証を無効にしなければならない。

（７） サーバルームへの入退室は記録しなければならない。

（８） サーバルーム内で長時間作業を行う場合は一人では実施せず、必ず同伴者を伴わなければならない。

（９） サーバルーム内で許可なく撮影・録音を行ってはならない。

（１０）サーバルームには作業に必要のないものを置いてはならない。もし置いてあった場合は速やかに撤去しなければならない。

（１１）サーバルーム内の環境（機器・設備の有無、配置、利用状況等）は定期的に点検しなければならない。

（１２）その他のサーバルームの運用については『物理的対策標準』でのセキュリティ区画の扱いに準ずる。

３．５　例外事項

業務都合等により本標準の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

３．６　罰則事項

本標準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『罰則に関する標準』に従う。

３．７　公開事項

本標準は対象者にのみ公開するものとする。

３．８　改訂

・本標準は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本標準の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本標準は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

＊＊＊ 用語 ＊＊＊
機器と設備：設備は動かせないレベルのものを想定する。
機器・設備の重要度：「機器・設備が取扱う情報資産の重要度」と考える。情報資産の重要度については別途定める。
従業員：正社員以外の通常勤務しているスタッフも含むものと考える。